Cloud Computing:

Security Considerations and Recommendations for Agencies

Contents

Executive Summary

Many commercial organizations offer technology services ranging from hardware and software elements to network and infrastructure. The use of cloud services can relieve an agency that needs technology resources from having to acquire, develop, implement, and manage hardware and software with which they are unfamiliar. Furthermore, the use of a cloud provider may seem considerably less expensive, an important factor during changing economic times.

However, the factor that must be considered in evaluating the total cost of using cloud services is the importance of protecting agency data from loss, destruction and inappropriate disclosure. The agency always retains the full responsibility for the safekeeping of its information, and for determining the amount of risk it is willing to incur in the process.

This document was developed to help the agencies examine security controls to be considered when evaluating the use of cloud computing services.

Cloud Computing Defined

The National Institute for Standards and Technology Special Publication SP800-145 defines cloud computing as a model for enabling universal, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management efforts or service provider interaction. We have adopted this definition for our purposes, as well.

This cloud model is composed of five essential characteristics, three service models and four deployment models.

Essential Characteristics:

On-demand self-service: A service in which individuals may enroll themselves without assistance.

Broad Network Access: A service that is made available through standard Internet-enabled devices (e.g. mobile phones, tablets, laptops, and workstations).

Resource Pooling: Processing and storage demands that are balanced across a common infrastructure with no particular resource assigned to any individual user; resources are organized into a pool which can be accessed and used on demand. Therefore, as soon as one user releases a resource, it becomes available to another user. This arrangement increases the capacity of the system and allows for better capacity-utilization of resources.

Rapid Scalability: A feature which allows users to increase or decrease their resource capacity at will and according to their needs.

Measured Service: A type of cloud computing service wherein users are charged a fee based on a combination of the computing power, bandwidth and/or storage used. Since it is measured, resource usage can be monitored, controlled and reported in increments.

Service Models

Software as a Service (SaaS): A service that offers the provider's application software running on a cloud infrastructure. Software supplied via the cloud is often easy to use and requires little intervention from the users to get the service up and running. The service provider is responsible for software upgrades and maintenance.

Platform as a Service (PaaS): In computing, a platform refers to the hardware and software framework that allows applications to execute. Users rent infrastructure and programming tools hosted by the provider to create their own applications. The provider is responsible for maintaining the supporting hardware and software.

Infrastructure as a Service (IaaS): Computing infrastructure includes the servers, wires, cooling system and all the other resources necessary to run a data center. IaaS allows the user to provision processing, storage, networks, and other fundamental computing resources to allow the user to deploy and execute software, including operating systems and applications.

Deployment Models

Public Cloud: A cloud made available for the use of the general public –the most common type of cloud.

Community Cloud: A cloud made available to a certain group of individuals for their exclusive use. It may be owned, managed and operated by one or more organizations in the community or by a third party provider, or by a combination of both.

Private Cloud: A cloud made available to only one particular organization. It may be owned, managed and operated by one or more organizations in the community, by a third party provider, or by a combination of both.

Hybrid Cloud: A combination of two or more of the other cloud deployment models that are bound together by standardized technology, and which enable data and application portability.

Data Protection Required

The data used to satisfy the mission of an agency must be considered an asset, and therefore must be protected from loss, destruction, and inappropriate disclosure.

Certain steps must be taken to ensure the appropriate level of security is used depending on the sensitivity and classification of the agency data. More controls will be required if the data has been classified as sensitive than if it is considered public information. Once the data classification has been

completed, the System Owner must determine how best to safeguard the information through the use of physical and logical access controls.

Since requirements and conditions may change, it is recommended that any service being used is under the control of a written contract to protect the agency.

Systems containing sensitive data should include the highest level of appropriate controls based on the confidentiality and integrity of the data. These controls may include:

1. Encryption of the data prior to sending to cloud
2. Use of a managed Private Cloud
3. Elimination of Cloud storage as an option; keep the system in-house

If the system includes data that is sensitive with respect to confidentiality, the agency should strongly consider not using a Cloud based service.

Process Description

Business Impact Analysis and Data Classification

The potential for data loss or data exposure is increased by the action of moving agency information across a network to the cloud provider. Therefore, prior to contracting for cloud services, the agency must conduct a Business Impact Analysis (BIA) in order to understand and document the potential effects on the agency and its missions if data loss or data exposure were to occur. The BIA conducted for this purpose must satisfy the requirements of ITRM Information Security Standard, known as SEC501. Of particular importance are Sections 3. Business Impact Analysis and 4. IT System and Data Sensitivity Classification for any data to be stored, processed, or moved to or from the provider.

Control Requirements Identified

Based on the results and recommendations of the BIA and data classification study, control requirements must be established to meet the requirements of SEC501 in order to protect the agency's information. The following table identifies the minimum recommended control areas and the party responsible for maintaining each. ***Even though the cloud service provider may be identified as the party responsible for maintaining the control area, the agency is always ultimately responsible for determining that the control is implemented and maintained in a way sufficient to keep the data safe.***

Control Area	SaaS	PaaS	IaaS
Information Security Roles and Responsibilities	Agency and/or Provider	Agency and/or Provider	Agency and/or Provider
Risk Assessment	Agency	Agency	Agency

IT Security Audits	Agency Audit Division, APA, and other audit obligations	Agency Audit Division, APA, and other audit obligations	Agency Audit Division, APA, and other audit obligations
Contingency Planning	Agency and/or Provider	Agency and/or Provider	Agency and/or Provider
Continuity of Operations Planning	Agency	Agency	Agency
IT Disaster Recovery Planning Documentation	Agency and/or Provider	Agency and/or Provider	Agency and/or Provider
IT System and Data Backup and Restoration	Provider	Provider	Agency and/or Provider
Information Systems Security			
System Security Plans	Agency	Agency	Agency
System Hardening	Provider	Provider	Agency and/or Provider
Malicious Code Protection	Provider	Provider	Agency and/or Provider
Systems Development Life Cycle Security	Provider	Provider	Agency
Application Security	Provider	Provider	Agency
Wireless Security	Provider	Provider	Agency and/or Provider
Logical Access Control			
Account Management	Agency and/or Provider	Agency and/or Provider	Agency and/or Provider
Password Management	Agency and/or Provider	Agency and/or Provider	Agency and/or Provider
Remote Access	Agency and/or Provider	Agency and/or Provider	Agency and/or Provider
Data Protection			
Data Storage Media Protection	Provider	Provider	Agency and/or Provider
Encryption	Agency and/or Provider	Agency and/or Provider	Agency and/or Provider
Data Destruction	Provider	Provider	Agency and/or Provider
Facilities Security			
Facilities Security	Provider	Provider	Provider
Personnel Security			
Access Determination and Control	Provider	Provider	Agency and/or Provider
Information Security Awareness and Training	Provider	Provider	Agency and/or Provider
Acceptable Use of Technological Resources	Provider	Provider	Agency and/or Provider
Email Communications	Provider	Provider	Agency and/or Provider
Threat Management			
Threat Detection	Provider	Provider	Agency and/or Provider
Information Security Monitoring and	Provider	Provider	Agency and/or

Logging			Provider
Information Security Incident Handling	Agency and/or Provider	Agency and/or Provider	Agency and/or Provider
Data Breach Notification	Provider	Provider	Agency and/or Provider
IT Asset Management			
Software License Management	Provider	Provider	Agency
Configuration Management and Change Control	Provider	Provider	Agency and/or Provider
International Legal			
Physical storage locations	Provider	Provider	Provider

Other Considerations

For each of these control areas, an analysis of security controls must be provided, demonstrating compliance with agency and Commonwealth security policies.

An interoperability agreement must be created, and the Provider must be responsible for implementing the controls specified.

System and Data owners must review the interoperability agreement to document policy, compliance and control deficiencies.

If the system is classified as "Sensitive," a Sensitive System Security Plan must be developed and approved by the System Owner in accordance with SEC501. The agency may consider creating their own compensating controls for identified deficiencies in control areas. For example, if a cloud Provider does not provide disaster recovery services for a system that requires critical availability, the agency can implement a local (non-cloud) data backup process to satisfy the availability control requirement as an alternative to sourcing another Provider.

As with all purchasing, follow the Virginia Public Procurement Act and all other applicable purchasing requirements.

References and Additional Reading

Educause has cloud computing resources for educational institutions:

http://www.educause.edu/Resources/Browse/Cloud+Computing/27148

NIST Special Publication 800-291 is the NIST Cloud Computing Standards Roadmap:

http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909024

NIST Special Publication SP800-146 is the Cloud Computing Synopsis and Recommendations:

http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

The Federal Risk and Authorization Management Program (FedRAMP) is a federal government program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

http://www.gsa.gov/portal/category/102371

An Info Security Magazine article emphasizing governance in a cloud migration strategy:

http://www.infosecurity-magazine.com/view/23946/comment-governance-is-key-to-managing-cloud-risk-/

A Network World article warning of the dangers of placing too much trust in your cloud service provider:

http://www.networkworld.com/news/2012/052512-cloud-security-gartner-259627.html?hpg1=bn&source=NWWNLE_nlt_cloud_security_2012-05-29

An article from SANS giving insight into the concerns about moving towards the cloud:

http://www.sans.org/cloud/2012/07/19/can-i-outsource-my-security-to-the-cloud

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing.

https://cloudsecurityalliance.org/